

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, James V. Richardson, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, and the transfer of obscene material to minors, including but not limited to, violations of 18 U.S.C. §§ 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Samuel E. MAIGRET (DOB XX/XX/1996) for possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). I submit this affidavit in support of applications to search

- a. the person of Samuel E. MAIGRET, date of birth 03/04/1996 (hereinafter “MAIGRET” and/or the “SUBJECT PERSON”), and
- b. MAIGRET’s residence, the premises located at 413 Grand Ave, Pawtucket, RI 02861 (the “SUBJECT PREMISES”)

and the content of any electronic media storage devices or media located on the SUBJECT PERSON or in the SUBJECT PREMISES, as more fully described in Attachments A-1 and A-2, which are incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachments B-1 and B-2, which is also incorporated herein by reference.

**BACKGROUND ON TOR AND BITCOIN**

3. Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user’s communications through a globally

distributed network of relay computers, or proxies, rendering conventional Internet Protocol (“IP”) address-based methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user’s web browser or by downloading the free “Tor browser bundle,” which is available at [www.torproject.org](http://www.torproject.org). When a Tor user accesses a website, only the IP address of the last relay computer (the “exit node”), as opposed to the user’s actual IP address, appears on the website’s IP address log. Currently, there is no practical method to trace a user’s actual IP address back through those Tor relay computers.

4. The Tor Network also makes it possible for users to operate websites, called “hidden services,” in a manner that conceals the true IP address of the computer hosting the website. Like other websites, “hidden services” are hosted on computer servers that communicate through IP addresses. However, hidden services bear some unique technical features that conceal the computer server’s location. As distinguished from standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, such as “asdlk8fs9dfku7f,” followed by the suffix “.onion.” Ordinarily, it is possible for investigators to determine the IP address of the computer server hosting a website through a simple public lookup via a Domain Name System (“DNS”) listing. Unlike ordinary Internet websites, there is no publicly available query that may be performed via a DNS listing to determine the IP address of the computer server that hosts a Tor hidden service. Although law enforcement agents may be able to view and access hidden services that are facilitating illegal activity, the IP address of a Tor hidden service cannot be determined via public lookups. Moreover, communications between users’ computers and a Tor hidden service web server are routed – as with all Tor communications – through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can determine the true IP address – and therefore the location – of the computer server that hosts a hidden service through public lookups or ordinary investigative means.

5. Bitcoin (“BTC”) is a type of virtual currency, circulated over the internet. BTC are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. BTC is just one of many varieties of virtual currency.

6. BTC are sent to and received from BTC “addresses.” A BTC address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long

case-sensitive string of letters and numbers. Each BTC address is controlled through the use of a unique corresponding private key – which is a cryptographic equivalent of a password or pin needed to access the address. Only the holder of an address’ private key can authorize any transfers of BTC from that address to other BTC addresses. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for each and every transaction.

7. To acquire BTC, a typical user will purchase them from a BTC virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (e.g., U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information of their customers and verify their clients’ identities.

8. To transfer BTC to another address, the sender transmits a transaction announcement, which is cryptographically signed with the sender’s private key, across the peer-to-peer BTC network. The BTC address of the receiving party (who has a private key) and the sender’s private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. Once the sender’s transaction announcement is verified by the network, the transaction is added to the blockchain – which is a decentralized public ledger that records all BTC transactions. The blockchain logs every BTC address that has ever received a BTC and maintains records of every transaction for each BTC address.

9. While the identity of a BTC address owner is generally anonymous (unless the owner opts to make information about the owner’s BTC address publicly available), analysis of the blockchain can often be used to identify the owner of a particular BTC address. Since the blockchain serves as a searchable public ledger of every BTC transaction, investigators may trace transactions to BTC exchangers. Because those exchangers generally collect identifying information about their customers, subpoenas or other appropriate process submitted to these

exchangers can, in some instances, reveal the true identity of an individual responsible for a BTC transaction.

10. Analysis of the blockchain can also, in some instances, reveal whether additional BTC addresses are controlled by the same individual or entity. For example, the proprietor of a website that accepts payment via BTC may create many BTC addresses in order to receive payments from different customers. If the proprietor decides to consolidate the BTC that it has received from those customers, the proprietor may group those many BTC addresses together in order to send a single transaction into one BTC account. Each of those many BTC addresses would then appear as “inputs” on a single transaction on the blockchain. Examining the transactions associated with a known BTC address may therefore reveal the existence of other BTC addresses that appeared as “inputs” alongside the known address – which indicates that the addresses were controlled by the same user. Additional examination of those BTC addresses and their activity on the blockchain may reveal further information about the user and his/her previous transactions.

11. Law enforcement uses sophisticated commercial services offered by several different blockchain analysis companies to investigate bitcoin transactions. These companies analyze the blockchain in an attempt to identify individuals or groups involved with bitcoin transactions. Specifically, these companies create large databases that group bitcoin transactions into “clusters” through analysis of data underlying bitcoin transactions. The service allows law enforcement to identify BTC addresses that are included as “inputs” in the same transaction, as described above, and “cluster” these addresses together. Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable.

12. This third-party blockchain analysis software is an anti-money laundering software used by banks and law enforcement organizations worldwide. It has supported many investigations and been the basis for numerous search and seizure warrants. As such, law enforcement has found the information provided by it to be reliable. Further, computer scientists have independently shown that they can use “clustering” methods to analyze clues in how bitcoins are typically aggregated or split up to identify BTC addresses and their respective account owners.

### **PROBABLE CAUSE AND BACKGROUND OF THE INVESTIGATION**

13. In August 2021, Homeland Security Investigations (HSI) Providence received an investigative referral from the HSI Cyber Crimes Center (C3) through the HSI Boston, MA office. The referral originated from a German Federal Criminal Police Office (BKA) investigation into the Tor-Hidden-Service "Teen World" utilizing the URL `teen7tfmwtpsbfk3.onion` and the Tor-Hidden-Service "365 CP" utilizing the URL `365c7q5jvm5c5rbz.onion`.

14. The websites referenced in the above paragraph advertise child sexual abuse material (CSAM) and offer CSAM for a payment in Bitcoin, Ethereum and Litecoin. On the start page of the websites, users can already view CSAM. However, to gain full access to the website users need to create an account and make a payment with one of the cryptocurrencies. If users want to pay with Bitcoin, the amount users had to pay is 0.0024 BTC to the BTC-address "1D3aQThytRGxD8xHefdhmvJqnMvHa55qhc" (as of 10.09.2020), although the BTC-address has changed since that time. After a successful payment, user accounts will be unlocked according to the instructions on the website.

15. In November 2020, the BKA served legal process to the Digital Currency Exchange (DCE) ("Coinbase") requesting information on users who used their Coinbase accounts to send payment to access the above websites. The response from Coinbase revealed that there were payments to the BTC-address from users located in the United States. Coinbase returned the following information on a user who purchased access to the above websites using his Coinbase account:

User ID: 5c2d853b5026990ef97a7ec5  
Name: Samuel Maigret  
Email: samuelmaigret@yahoo.com  
Phone: 508-431-3581  
Address: 11 Cherry Tree Lane, North Attleboro, MA 02760

16. Yahoo records obtained by HSI for the email address samuelmaigret@yahoo.com list the username as Samuel Maigret, and a recovery phone number of 508-431-3581, the same phone number listed in the Coinbase account above.

17. In May 2021, HSI/C3 sent the above information to the HSI Boston, MA office. HSI Boston began to investigate MAIGRET and discovered that he moved to Pawtucket, RI

since the purchase to access the above websites. HSI Boston then forwarded the lead to HSI Providence.

18. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Samuel E. MAIGRET. These public records indicated that MAIGRET currently resides at 413 Grand Ave, Pawtucket, RI 02861. The database indicates that MAIGRET previously resided at 11 Cherry Tree Lane, North Attleboro, MA 02760. The database also revealed that MAIGRET's phone number is 508-431-3581 (the same phone number provided by Coinbase).

19. In August 2021, the U.S. Postal Service confirmed that Samuel E. MAIGRET is currently receiving mail at the SUBJECT PREMISES.

20. On August 17, 2021, physical surveillance of the SUBJECT PREMISES was conducted. The SUBJECT PREMISES appears to be a unit in a multi-family apartment building, yellow in color. There are 2 doors and two mailboxes in the front of the house. The mailbox next to the right front door has the number "413" clearly affixed to the house directly above the mailbox.

21.

**CHARACTERISTICS COMMON TO PERSONS WHO ENGAGE IN  
CHILD SEXUAL EXPLOITATION**

22. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct, or who engage in sexually explicit communications with minors. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

23. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

24. Such offenders may collect sexually explicit or suggestive materials in a variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual

interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

25. Such offenders almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their cache for many years. In my training and experience, I am aware that such offenders often

26. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a, “SD card,” computer or surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the offender’s residence, inside the offender’s vehicle, or, at times, on his person, to enable the individual to view the child pornography images, which are highly valued.<sup>1</sup>

27. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.<sup>2</sup>

28. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material,

---

<sup>1</sup> See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections);

<sup>2</sup> See *United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).



and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography.

29. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if such an offender uses a portable device (such as a mobile phone or gaming device) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home – here, the SUBJECT PREMISES, as set forth in Attachment A-2.

30. Based upon the foregoing, I believe that Samuel E. MAIGRET likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. As such, I submit that there is probable cause to believe that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of possession and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252(a)(4) (B) and (b)(2) exist at the SUBJECT PREMISES.

#### **SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA**

31. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used,



what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

32. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

a. The volume of evidence: Storage media such as hard disks, SD cards, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected,

or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

### **BIOMETRIC ACCESS TO DEVICES**

33. This warrant permits law enforcement to compel Samuel E. MAIGRET to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes, and records data based on

the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such

features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

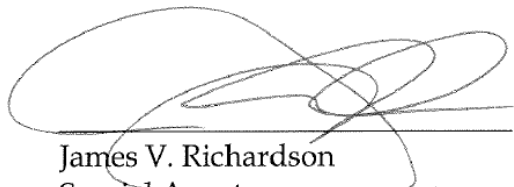
- h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Samuel E. MAIGRET to the fingerprint scanner of the DEVICES found at the premises; (2) hold the DEVICES found at the premises in front of the face of Samuel E. MAIGRET and activate the facial recognition feature; and/or (3) hold the DEVICES found at the premises in front of the face of Samuel E. MAIGRET and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Samuel E. MAIGRET state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Samuel E. MAIGRET to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

**CONCLUSION**

34. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B-1 and Attachment B-2, are located on the person and at the locations described in Attachment A-1 and Attachment A-2. I respectfully request that this Court issue search warrants for the locations described in Attachment A-1 and Attachment A-2, authorizing the seizure and search of the items described in Attachment B-1 and Attachment B-2, respectively.

35. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Sworn to under the pains and penalties of perjury,

  
James V. Richardson  
Special Agent  
Homeland Security

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1  
by:

\_\_\_\_\_ telephone \_\_\_\_\_  
(specify reliable electronic means)

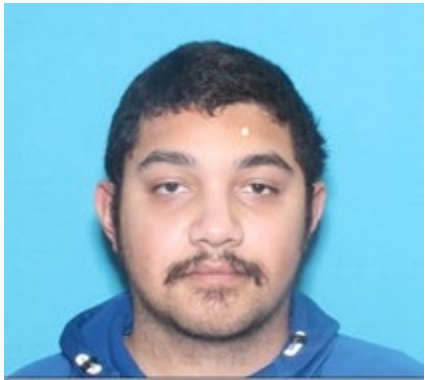
\_\_\_\_\_  
Date  
  
Providence, Rhode Island  
City and State

\_\_\_\_\_  
Judge's signature  
  
Lincoln D. Almond, US Magistrate Judge  
Printed name and title

**ATTACHMENT A-1**

**DESCRIPTION OF PERSON TO BE SEARCHED**

The person of Samuel E. MAIGRET, a male, standing approximately 5'05", date of birth 03/04/1996 (the SUBJECT PERSON).



The search shall include the content of any electronic media storage devices, including smart phones, or media located on the person of Samuel E. MAIGRET, regardless of the location at which he may be found.

**ATTACHMENT B-1**  
**DESCRIPTION OF INFORMATION TO BE SEIZED<sup>3</sup>**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

---

<sup>3</sup> For the purpose of this warrant, and attachments thereto:

A. "Records" and "information" may be any collection of data or information, including communications. A record may be comprised of letters, numbers, pictures, sounds or symbols. Records and information include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

B. "Computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

C. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

D. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

E. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a username; or a password), whether stored deliberately, inadvertently, or automatically.

F. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

G. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

H. "Storage medium" and/or "storage media" includes any physical object upon which computer data can be recorded, collected, retrieved, and/or transmitted, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, DVDs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

I. "Obscene material" is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.



- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this

attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
  - a. Records, information, and items relating to the occupancy or ownership of the 413 Grand Ave, Pawtucket, RI 02861 (SUBJECT PREMISES), including utility and telephone bills, mail envelopes, or addressed correspondence;
  - b. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes;
  - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
  - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

During the execution of the search of the SUBJECT PERSON described in Attachment A-1 and the SUBJECT PREMISES described in Attachment A-2, law enforcement personnel are also specifically authorized to compel the SUBJECT PERSON, Samuel E. MAIGRET, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found on the SUBJECT PERSON and any of the DEVICES found at the SUBJECT PREMISES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Samuel E. MAIGRET to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

**ATTACHMENT A-2**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The premises to be searched include:

The Premises located at 413 Grand Ave, Pawtucket, RI 02861, more particularly described as a unit within a yellow multi-family apartment building. The number “413” is clearly marked above the mailbox to the right of the front door to the right. The building containing the SUBJECT PREMISES also contains another unit, 415 Grand Avenue, Pawtucket, RI. The exterior of the premises is pictured below:



**ATTACHMENT B-2**

**DESCRIPTION OF INFORMATION TO BE SEIZED<sup>4</sup>**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

---

<sup>4</sup> For the purpose of this warrant, and attachments thereto:

A. "Records" and "information" may be any collection of data or information, including communications. A record may be comprised of letters, numbers, pictures, sounds or symbols. Records and information include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

B. "Computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

C. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

D. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

E. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a username; or a password), whether stored deliberately, inadvertently, or automatically.

F. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

G. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

H. "Storage medium" and/or "storage media" includes any physical object upon which computer data can be recorded, collected, retrieved, and/or transmitted, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, DVDs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

I. "Obscene material" is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this

attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
  - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;
  - b. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes;
  - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
  - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

During the execution of the search of the SUBJECT PREMISES described in Attachment A-2, law enforcement personnel are also specifically authorized to compel the SUBJECT PERSON, Samuel E. MAIGRET, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found on the SUBJECT PERSON and any of the DEVICES found at the SUBJECT PREMISES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant.



This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Samuel E. MAIGRET to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.